Interference Search 09/823179

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"public key".clm. and "private key".clm. and "digital signatuure".clm. and authenticat$3.clm. and database.clm. and account$1.clm. and device.clm. and identifier.clm. and generat$3.clm.	US-PGPUB; USPAT	OR	OFF	2005/12/15 17:27
L2	21	"public key".clm. and "private key".clm. and "digital signature".clm. and authenticat$3.clm. and database.clm. and account$1.clm. and device.clm. and identifier.clm. and generat$3.clm.	US-PGPUB; USPAT	OR	OFF	2005/12/15 17:27

updated search 09/923179

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"public key".clm. and "private key".clm. and "digital signatuure". clm. and authenticat$3.clm. and database.clm. and account$1.clm. and device.clm. and identifier.clm. and generat$3.clm.	US-PGPUB; USPAT	OR	OFF	2005/12/15 17:27
L2	21	"public key".clm. and "private key".clm. and "digital signature". clm. and authenticat$3.clm. and database.clm. and account$1.clm. and device.clm. and identifier.clm. and generat$3.clm.	US-PGPUB; USPAT	OR	OFF	2005/12/15 17:28
L3	1185	"public key" and "private key" and "digital signature" and authenticat$3 and database and account$1 and device and identifier and generat$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/12/15 17:28
L4	1050	713/182	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/12/15 17:29
L5	4657	713/182 or 713/172 or 713/176 or 713/169 or 380/282 or 380/285 or 705/64 or 705/67	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/12/15 17:30
L6	191	5 and 3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/12/15 17:30
L7	157	6 and authority	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/12/15 17:30

09/923,179

Terms used **public key** and **private key** and **digital signature** and **authenticat$3** and **database** and **account$1** and **device** and **identifier** and **generat$3**

Found **1,507** of **167,655**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Applications: Context sensitive access control

R. J. Hulsebosch, A. H. Salden, M. S. Bargh, P. W. G. Ebben, J. Reitsma

June 2005 **Proceedings of the tenth ACM symposium on Access control models and technologies**

Publisher: ACM Press

Full text available: pdf(145.62 KB) Additional Information: full citation, abstract, references, index terms

We investigate the practical feasibility of using context information for controlling access to services. Based solely on situational context, we show that users can be transparently provided anonymous access to services and that service providers can still impose various security levels. Thereto, we propose context-sensitive verification methods that allow checking the user's claimed authenticity in various ways and to various degrees. More precisely, conventional information management approac ...

Keywords: access control, authentication, context sensitive, context verification, service usage patterns

2 Crypto-based identifiers (CBIDs): Concepts and applications

Gabriel Montenegro, Claude Castelluccia

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(262.76 KB) Additional Information: full citation, abstract, references, index terms, review

This paper addresses the identifier ownership problem. It does so by using characteristics of Statistical Uniqueness and Cryptographic Verifiability (SUCV) of certain entities which this document calls SUCV Identifiers and Addresses, or, alternatively, Crypto-based Identifiers. Their characteristics allow them to severely limit certain classes of denial-of-service attacks and hijacking attacks. SUCV addresses are particularly applicable to solve the address ownership problem that hinders mechani ...

Keywords: Security, address ownership, authorization, group management, mobile IPv6, opportunistic encryption

3 Authentication in distributed systems: theory and practice

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4
Publisher: ACM Press

Full text available: pdf(3.37 MB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegated authority. The theory shows how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We ...

Keywords: certification authority, delegation, group, interprocess communication, key distribution, loading programs, path name, principal, role, secure channel, speaks for, trusted computing base

4 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure

Albert Levi, M. Ufuk Caglayan, Cetin K. Koc
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press

Full text available: pdf(532.64 KB) Additional Information: full citation, abstract, references, index terms, review

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called public key infrastructure (PKI), and verify the certificates on this path recursively. This is classical methodology. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is to issue special certificates (called nested certificates) for other certifica ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

5 DRM experience: Digital rights management in a 3G mobile phone and beyond

Thomas S. Messerges, Ezzat A. Dabbish
October 2003 **Proceedings of the 2003 ACM workshop on Digital rights management**
Publisher: ACM Press

Full text available: pdf(306.59 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

6 Authentication in distributed systems: theory and practice

Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber

September 1991 **ACM SIGOPS Operating Systems Review , Proceedings of the thirteenth ACM symposium on Operating systems principles SOSP '91**, Volume 25 Issue 5

Publisher: ACM Press

Full text available: pdf(2.33 MB) Additional Information: full citation, abstract, references, citings, index terms

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegation of authority. The theory explains how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We use the th ...

7 Multi-agent systems and social behavior: A user-centric anonymous authorisation framework in e-commerce environment

Richard Au, Harikrishna Vasanta, Kim-Kwang Raymond Choo, Mark Looi

March 2004 **Proceedings of the 6th international conference on Electronic commerce ICEC '04**

Publisher: ACM Press

Full text available: pdf(291.06 KB) Additional Information: full citation, abstract, references

A novel user-centric authorisation framework suitable for e-commerce in an open environment is proposed. The credential-based approach allows a user to gain access rights anonymously from various service providers who may not have pre-existing relationships. Trust establishment is achieved by making use of referrals from external third parties in the form of *Anonymous Attribute Certificates.* The concepts of *One-task Authorisation Key* and *Binding Signature* are proposed to fac ...

8 SPV: secure path vector routing for securing BGP

Yih-Chun Hu, Adrian Perrig, Marvin Sirbu

August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

9 Formal prototyping in early stages of protocol design

Alwyn Goodloe, Carl A. Gunter, Mark-Oliver Stehr

January 2005 **Proceedings of the 2005 workshop on Issues in the theory of security**

Publisher: ACM Press

Full text available: pdf(530.03 KB) Additional Information: full citation, abstract, references

Network protocol design is usually an informal process where debugging is based on successive iterations of a prototype implementation. The feedback provided by a

prototype can be indispensable since the requirements are often incomplete at the start. A draw-back of this technique is that errors in protocols can be notoriously difficult to detect by testing alone. Applying formal methods such as theorem proving can greatly increase one's confidence that the protocol is correct. However, formal m ...

10 Public-key support for group collaboration

Carl Ellison, Steve Dohrmann

November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4

Publisher: ACM Press

Full text available: pdf(561.61 KB) Additional Information: full citation, abstract, references, index terms

This paper characterizes the security of group collaboration as being a product not merely of cryptographic algorithms and coding practices, but also of the man-machine process of group creation. We show that traditional security mechanisms do not properly address the needs of a secured collaboration and present a research prototype, called NGC (next generation collaboration), that was designed to meet those needs. NGC distinguishes itself in the care with which the man-machine process was analy ...

Keywords: Human-computer interface, IPsec, PGP, PKI, S/MIME, SDSI, SPKI, SSH

11 Astrolabe: A robust and scalable technology for distributed system monitoring, management, and data mining

Robbert Van Renesse, Kenneth P. Birman, Werner Vogels

May 2003 **ACM Transactions on Computer Systems (TOCS)**, Volume 21 Issue 2

Publisher: ACM Press

Full text available: pdf(341.62 KB) Additional Information: full citation, abstract, references, citings, index terms

Scalable management and self-organizational capabilities are emerging as central requirements for a generation of large-scale, highly dynamic, distributed applications. We have developed an entirely new distributed information management system called Astrolabe. Astrolabe collects large-scale system state, permitting rapid updates and providing on-the-fly attribute aggregation. This latter capability permits an application to locate a resource, and also offers a scalable way to track sys ...

Keywords: Aggregation, epidemic protocols, failure detection, gossip, membership, publish-subscribe, scalability

12 An architecture for secure wide-area service discovery

Todd D. Hodes, Steven E. Czerwinski, Ben Y. Zhao, Anthony D. Joseph, Randy H. Katz

March 2002 **Wireless Networks**, Volume 8 Issue 2/3

Publisher: Kluwer Academic Publishers

Full text available: pdf(365.68 KB) Additional Information: full citation, abstract, references, citings, index terms

The widespread deployment of inexpensive communications technology, computational resources in the networking infrastructure, and network-enabled end devices poses an interesting problem for end users: how to locate a particular network service or device out of hundreds of thousands of accessible services and devices. This paper presents the architecture and implementation of a secure wide-area Service Discovery Service (SDS). Service providers use the SDS to advertise descriptions of available ...

Keywords: location services, name lookup, network protocols, service discovery

13 The Ω key management service

Michael K. Reiter, Matthew K. Franklin, John B. Lacy, Rebecca N. Wright

January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

14 Revokable and versatile electronic money (extended abstract)

Markus Jakobsson, Moti Yung

January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.53 MB) Additional Information: full citation, references, citings, index terms

15 Architecture for Protecting Critical Secrets in Microprocessors

Ruby B. Lee, Peter C. S. Kwan, John P. McGregor, Jeffrey Dwoskin, Zhenghong Wang

June 2005 **Proceedings of the 32nd Annual International Symposium on Computer Architecture ISCA '05**

Publisher: IEEE Computer Society

Full text available: pdf(143.62 KB) Additional Information: full citation, abstract

We propose "secret-protected (SP)" architecture to enable secure and convenient protection of critical secrets for a given user in an on-line environment. Keys are examples of critical secrets, and key protection and management is a fundamental problem ¿ often assumed but not solved ¿ underlying the use of cryptographic protection of sensitive files, messages, data and programs. SP-processors contain a minimalist set of architectural features that can be built into a general-purpose microprocess ...

16 Data integrity: The HP time vault service: exploiting IBE for timed release of confidential information

Marco Casassa Mont, Keith Harrison, Martin Sadler

May 2003 **Proceedings of the 12th international conference on World Wide Web**

Publisher: ACM Press

Full text available: pdf(860.87 KB) Additional Information: full citation, abstract, references, index terms

Digital information is increasingly more and more important to enable interactions and transactions on the Internet. On the other hand, leakages of sensitive information can have harmful effects for people, enterprises and governments.This paper focuses on the problems of dealing with timed release of confidential information and simplifying its access once public: it is a common issue in the industry, government and day-to-day life.We introduce the "HP Time Vault Service", based on the emerging ...

Keywords: disclosure policies, identifier-based encryption, privacy, security, timed-release, web service

17 User interface requirements for authentication of communication

Audun Jøsang, Mary Anne Patton

February 2003 **Proceedings of the Fourth Australian user interface conference on User interfaces 2003 - Volume 18 CRPITS '03**

Publisher: Australian Computer Society, Inc.

Full text available: pdf(375.46 KB) Additional Information: full citation, abstract, references, index terms

Authentication is a security service that consists of verifying that someone's identity is as claimed. There are a number of challenges to presenting information from the authentication process to the user in a way that is meaningful and ensures security. We show examples where authentication requirements are not met, due to user behaviour and properties of existing user interfaces, and suggest some solutions to these problems.

Keywords: authentication, non-repudiation, security, usability, user interface

18 Untraceability in mobile networks

Didier Samfat, Refik Molva, N. Asokan

December 1995 **Proceedings of the 1st annual international conference on Mobile computing and networking**

Publisher: ACM Press

Full text available: pdf(1.20 MB) Additional Information: full citation, references, citings, index terms

Keywords: CDPD, GSM, alias, anonymity, authentication, location privacy, mobility, security

19 Applications, services, and architecture: Reputation-based Wi-Fi deployment protocols and security analysis

Naouel Ben Salem, Jean-Pierre Hubaux, Markus Jakobsson

October 2004 **Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots**

Publisher: ACM Press

Full text available: pdf(395.70 KB) Additional Information: full citation, abstract, references, index terms

In recent years, wireless Internet service providers (WISPs) have established thousands of WiFi hot spots in cafes, hotels and airports in order to offer to travelling Internet users access to email, web or other Internet service. However, two major problems still slow down the deployment of this kind of networks: the lack of a seamless roaming scheme and the variable quality of service experienced by the users. This paper provides a response to these two problems: We present a solution that, ...

Keywords: QoS, WiFi networks, billing, protocols, reputation systems, roaming, security

20 Standardizing information technology security

Warwick Ford

June 1994 **StandardView**, Volume 2 Issue 2

Publisher: ACM Press

Full text available: pdf(1.12 MB) Additional Information: full citation, references, index terms

Search Results

Results for "(((((public key and private key and digital signature <in>metadata))<and>(database&..." e-mail
Your search matched **5** of **5** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

(((((public key and private key and digital signature <in>metadata))<and>(databas

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Select Article Information

1. **Development of personal authentication system using fingerprint with di technologies**
Isobe, Y.; Seto, Y.; Kataoka, M.;
System Sciences, 2001. Proceedings of the 34th Annual Hawaii International C
Jan 3-6 2001 Page(s):9 pp.
AbstractPlus | Full Text: PDF(324 KB) IEEE CNF

2. **An Efficient Authentication Scheme with Fault Tolerance for Database Sy**
Zhang, C.N.; Chunren Lai; Honglan Zhong;
Information Technology and Applications, 2005. ICITA 2005. Third Internationa
Volume 2, 4-7 July 2005 Page(s):448 - 453
Digital Object Identifier 10.1109/ICITA.2005.62
AbstractPlus | Full Text: PDF(112 KB) IEEE CNF

3. **A case study of authenticated and secure file transfer: the Iowa Campaig Reporting System (iCFRS)**
Hastings, N.E.; Whitmer, J.M.; Davis, J.A.; Jacobson, D.W.;
Performance, Computing, and Communications Conference, 1997. IPCCC 19 International
5-7 Feb. 1997 Page(s):532 - 538
Digital Object Identifier 10.1109/PCCC.1997.581560
AbstractPlus | Full Text: PDF(692 KB) IEEE CNF

4. **A novel blind signature scheme possessed with dual protections**
Jen-Rong Chen, J.; An-Pin Chen; Wen-Mao Lin, R.;
Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Conference on
14-16 Oct. 2003 Page(s):123 - 127
Digital Object Identifier 10.1109/CCST.2003.1297547
AbstractPlus | Full Text: PDF(1393 KB) IEEE CNF

5. **Scalable and efficient PKI for inter-organizational communication**
Ansper, A.; Buldas, A.; Freudenthal, M.; Willemson, J.;
Computer Security Applications Conference, 2003. Proceedings. 19th Annual 2003 Page(s):308 - 318
Digital Object Identifier 10.1109/CSAC.2003.1254335
AbstractPlus | Full Text: PDF(311 KB) IEEE CNF